Leveraging Game Theory to Achieve Efficient Attack-aware Service Provisioning in EONs

Jing Zhu, Bin Zhao, Zuqing Zhu, *Senior Member, IEEE*

***Abstract*—Multi-domain elastic optical networks (MD-EONs) help to improve network scalability, extend service coverage, and facilitate good inter-operability to orchestrate administrative domains managed by different carriers. Since the users in other domains can launch cross-domain physical-layer attacks to a domain, this paper studies the problem of attack-aware service provisioning in one domain of an MD-EON. We consider a realistic scenario that does not treat all the inter-domain lightpaths as malicious ones, and try to arrange the lightpaths' routing and spectrum assignment (RSA) schemes with the help of game theory to balance the spectrum utilization and security-level of the domain well. Specifically, we define a two-player Bayesian game to represent the provisioning procedure for each inter-domain request, and design the game strategies and utility functions for the players (*i.e.*, the domain manager and the user from other domains). Then, we formulate a nonlinear programming (NLP) model, solve the game with it to obtain a Bayesian Nash equilibrium (BNE), and determine the best strategies for the players based on the BNE. Finally, with the game model, we propose a game-assisted RSA (Ga-RSA) algorithm to achieve attack-aware service provisioning efficiently. The proposed algorithm is evaluated with extensive simulations and the results confirm its effectiveness.**

***Index Terms*—Multi-domain elastic optical networks (MD-EONs), Bayesian game, Physical-layer security, Routing and spectrum assignment (RSA).**

I. Introduction

RECENTLY, due to the exponential increase of high-throughput and dynamic traffic demands in backbone networks, network operators' expectation on highly-efficient and flexible optical networking technologies is becoming more and more urgent. However, the traditional fixed-grid wavelength-division multiplexing (WDM) networks only have limited flexibility in the optical layer [1]. Under this circumstance, the elastic optical networks (EONs), which can allocate optical spectrum in a flexible-grid way and thus achieve agile bandwidth management in the optical layer, have attracted intensive interests recently [1]. Specifically, the bandwidth-variable transponders (BV-Ts) and bandwidth-variable wavelength selective switches (BV-WSS') in EONs operate on narrow-band frequency slots (FS') at 12.5 GHz or even less and groom them adaptively to realize both sub-wavelength and super-channel transmissions [2, 3].

Meanwhile, except for their appealing potential, EONs are still facing a few challenges. An important one of them is how to achieve efficient service provisioning in multi-domain EONs (MD-EONs). Since a backbone network usually covers a relatively large geographical area and can be managed by multiple network operators, the multi-domain scenario of EONs has to be addressed properly. Previously, people have considered the cross-domain orchestration in MD-EONs and proposed a few network architectures in [4–6]. These studies leveraged the idea of intra-domain topology virtualization to address the scalability and security issues in cross-domain service provisioning. Specifically, to support cross-domain service provisioning, a domain manager first abstracts the related path segments in its domain to obtain an intra-domain virtual topology (ID-VT) and then shares the ID-VT with either the peer domains or the high-level resource broker. Note that the ID-VT helps to protect the domain privacy and thus improves the physical-layer security within each domain. However, this is far from enough as malicious users can still launch physical-layer attacks from outside of the domain and put the intra-domain resources/requests in danger.

In optical networks, optical components, *e.g.*, fibers, amplifiers and cross-connects (OXCs), can be vulnerable to various physical-layer issues [7]. For example, the nonlinearity of fibers can cause inter-channel crosstalk, while the imperfect response of optical filters can result in intra-channel crosstalk in OXCs. Therefore, when multiple lightpaths share these components, they can affect one another's performance due to these issues and a physical-layer attack can be launched by a malicious user therein [8]. For instance, an eavesdropper can easily utilize the crosstalk to steal information with an unmodulated lightpath. This actually suggests that in MD-EONs, a domain manager should not fully trust the users that reside in other domains as they cannot be directly monitored or managed to avoid physical-layer attacks. More importantly, compared with those in WDM networks, the security threats in EONs can be more devastating since the channel spacing is much narrower and lightpaths can carry much more information due to the introduction of super-channels.

Note that a few measures can alleviate the aforementioned security threats. For example, we can build opaque domains by strictly enforcing optical-to-electrical-to-optical (O/E/O) conversions at domain edges. This, however, would remove the main purpose and benefits of multi-domain networking and increase both the capital expenditure (CAPEX) and operational expenditure (OPEX) of MD-EONs to an unacceptable level. Hence, in our previous work [9], we considered optically translucent domains and proposed several attack-aware service provisioning schemes to enhance the physical-layer security in MD-EONs cost-efficiently. More specifically, we tried to minimize the sharing of optical components between intra- and

J. Zhu, B. Zhao and Z. Zhu are with the School of Information Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, P. R. China (email: zqzhu@ieee.org).

Manuscript received on July 20, 2016.

inter-domain lightpaths and inserted spectral guard-bands to isolate their spectrum usages if the sharing cannot be avoided.

Even though the schemes we proposed in [9] are apparently more cost-efficient than the idea of building opaque domains, their efficiencies can still be improved. The schemes were developed based on the consideration that treats every inter-domain lightpath as a malicious one. Note that the basic premise for an MD-EON to operate normally is that most of its users should be harmless and trusted ones since this ensures the mutual trust among the domains. In other words, if a domain is resided with too many malicious users, we should treat it as a compromised one and quarantine it from other domains. Consequently, treating every inter-domain lightpath as a malicious one would lead to over-protection and make the service provisioning inefficient in terms of spectrum utilization. Therefore, it would be better if the domain manager could intelligently categorize inter-domain lightpaths into harmless and malicious ones based on the network status and then apply the corresponding routing and wavelength assignment (RSA) schemes on them. This actually motivates us to seek help from the game theory. Specifically, if we consider the domain manager and the users from other domains as the players in an attacker/defender game [10], we can leverage the Bayesian game to further improve the performance of attack-aware service provisioning.

In this paper, we still address the problem of attack-aware service provisioning in one domain of an MD-EON, which considers both inter- and intra-domain lightpaths, *i.e.*, using a network model that is similar as that in [9]. Nevertheless, we consider a more realistic scenario that does not treat all the inter-domain lightpaths as malicious ones, and try to arrange the lightpaths' RSA schemes with the help of game theory to balance the spectrum utilization and security-level of the domain better. Specifically, we define a two-player Bayesian game to represent the provisioning procedure for each inter-domain request, and design the game strategies and utility functions for the players (*i.e.*, the domain manager and the user from other domains). Then, we formulate a nonlinear programming (NLP) model, solve the game with it to obtain a Bayesian Nash equilibrium (BNE), and determine the best strategies for the players based on the BNE. With the game model, we propose a game-assisted RSA (Ga-RSA) algorithm to achieve attack-aware service provisioning efficiently. The proposed algorithm is evaluated with extensive simulations and the results confirm its effectiveness.

The rest of the paper is organized as follows. Section II provides a brief survey on the related work. The problem description is given in Section III, and in Section IV, we define the Bayesian game for serving an inter-domain request. The NLP model for solving the Bayesian game is formulated in Section V, where the overall procedure of Ga-RSA is also presented. Then, we discuss the performance evaluation in Section VI. Finally, Section VII summarizes the paper.

II. Related Work

With the assistance of attack and fault management, various technologies have been proposed and demonstrated to improve the physical-layer security of optical networks [11–15]. As they would require additional hardware elements, they are out of the scope of this work. For WDM networks, the authors of [16–19] proposed to perform careful network planning to minimize the damages induced by possible physical-layer attacks. Specifically, they formulated the problem of attack-aware routing and wavelength assignment (Aa-RWA) to consider different kinds of physical-layer attacks, and tried to optimize the routing scheme, the wavelength assignment scheme, or both of them jointly. However, these studies treated all the requests equally in Aa-RWA, while in multi-domain scenarios, the intra-domain and inter-domain requests should be handled differently.

To protect domain privacy in multi-domain networks, people have proposed several topology virtualization mechanisms in [20–22]. And the studies in [4–6, 23] have considered how to achieve efficient network orchestration in MD-EONs. However, the RSA schemes used in these studies were directly adapted from those designed for single-domain EONs [24–31]. This means that within each domain, inter-domain requests would be treated equally with intra-domain ones and thus the security threat that inter-domain requests could be exploited to launch cross-domain physical-layer attacks was not addressed. In our previous work in [9], we proposed to differentiate the RSA schemes of intra- and inter-domain requests with security considerations, for enhancing the physical-layer security-level of a domain in an MD-EON. Nevertheless, we only considered the worst case and treated every inter-domain lightpath as a malicious one. Specifically, we overlooked the fact that the basic premise for an MD-EON to operate normally is that most of the lightpaths in it should be harmless.

Game theory provides us a powerful mathematical tool to analyze the competition and cooperation among rational decision-makers, and thus has been widely used to solve the problems in various networks. In [32], Liu *et al.* modeled the security threat in wireless ad hoc networks as a Bayesian game and proposed a hybrid detection framework to address it. The authors of [33] leveraged a dynamic repeated game model to study the problem of spectrum pricing in cognitive radio networks. The work in [34] presented the Nash bargaining scheme for realizing inter-domain traffic engineering. The non-cooperative competition among service providers for lightpath services has been addressed in [35] for WDM networks. In [36], the authors modeled the problem of wavelength assignment as a strategic game and analyzed the the price of anarchy. For multi-domain WDM networks, Loja *et al.* [37] solved the inter-domain routing problem by finding the Nash equilibrium of the game between operators and customers. However, to the best of our knowledge, the game-assisted service provisioning towards enhanced security-level in physical-layer has not been explored for multi-domain optical networks before.

III. Problem Description

Note that, when two lightpaths share node(s) and/or link(s) and their spectrum assignments are spectrally overlapping or adjacent (referred to as adjacent lightpaths), there would be intra/inter-channel crosstalk between them [8]. In an MD-EON, such intra/inter-channel crosstalk in one domain can be leveraged by malicious users in other domains to launch physical-layer attacks, *e.g.*, power jamming or eavesdropping [9]. For instance, a malicious user can request an inter-domain lightpath without transmitting any data, and thus it can gather signal leakage from its adjacent lightpaths for eavesdropping. Since each domain in the MD-EON would handle its security issues independently, we only consider the non-cooperative game between the domain manager of one domain and the users in other domains. In the game of a certain domain, an inter-domain lightpath tries to access from an ingress node while the domain manager adopts a proper RSA algorithm to grant the corresponding optical transmission through its domain. Note that this consideration can practically fit into the known cross-domain orchestration schemes for MD-EONs [5]. For instance, in [5], an inter-domain lightpath is set up with the collaboration of multiple domains, where each related domain manager establishes the path segment in its own domain.

We use $\mathbf{G} = \{G^m(V^m, E^m), m \in [1, M]\}$ to denote the set of domain topologies in an MD-EON, where $G^m(V^m, E^m)$ is the topology of the m-th domain, and V^m and E^m represent the sets of nodes and bidirectional fiber links in G^m, respectively. $V_b^m \subset V^m$ is used to denote the set of border nodes in G^m, *i.e.*, the ingress/egress points for inter-domain lightpaths to go into/out of the domain. We assume that only the nodes in V_b^m are equipped with O/E/O converters, and an inter-domain lightpath can change its spectrum assignment in them if necessary. Within G^m, all the lightpaths are transmitted all-optically to save the cost and energy. In other words, we consider a translucent MD-EON here [38, 39]. Each $e \in E^m$ contains F FS', each of which has a bandwidth of 12.5 GHz to provide a capacity of $C_{\text{FS}} = 12.5$ Gb/s.

We categorize the lightpaths in G^m into three types, *i.e.*, R^{in}, R^{lv} and R^{ex}. Here, R^{in} represents intra-domain requests, and each of them has the form of $R_i^{in}(r, d, C)$, where i is its index, $r, d \in V^m$ are the source and destination, and C is the bandwidth requirement in Gb/s. The latter two types are for inter-domain lightpaths. R^{lv} are for those that originate from G^m but target to other domains. We use $R_i^{lv}(r, V_b^m, C)$ to represent a lightpath in this type, since it can use any border node in V_b^m to go out of G^m. R^{ex} are for the lightpaths from other domains, which will pass through or end in G^m. Such a lightpath can be denoted as $R_i^{ex}(V_b^m, d, C)$, whose ingress point is selected from V_b^m. Note that R^{ex} only contains the inter-domain lightpaths that would not experience O/E/O conversions at their ingress border nodes. The reason is that O/E/O conversions can eliminate the physical-layer security threats considered in this work, and thus the corresponding lightpaths become trusted ones that are equivalent to the lightpaths originating from the ingress border nodes. In other words, such lightpaths can be classified as R^{in} or R^{lv}, depending on whether their destinations are in G^m or not.

In the game, one player is the domain manager of G^m, denoting as q_m, while its opponent is a user in other domain, *i.e.*, q_{-m}. Here, the subscript "$-m$" means that the user can reside in any neighbor domain of G^m. Note that, as explained above, we only need to consider an external user as q_{-m} when it intends to set up a lightpath in R^{ex}. Then, q_{-m} can be either harmless or malicious. Specifically, if q_{-m} just tries to establish a harmless inter-domain lightpath, q_m should not waste its spectrum resources on quarantining its lightpath. Otherwise, if q_{-m} might try to launch an attack, it is malicious and thus should be quarantined, which can be realized with the special RSA arrangements developed in [9]. Due to the sporadicalness of cross-domain attacks, it would be reasonable to assume that among the lightpaths in R^{ex}, only a few would be malicious and can affect those in R^{in}. Since the lightpaths in R^{in} are under full control of the domain manager in G^m, we assume that they are all trusted and would not be leveraged to launch attacks. Hence, we should isolate them from those in R^{ex} that are malicious. For the lightpaths in R^{lv} and the harmless ones in R^{ex}, the domain manager q_m does not have to isolate them from the malicious ones in R^{ex}, and only try to improve their security-levels in a best-effort way. Specifically, these lightpaths can share optical components with the malicious ones in R^{ex} without proper isolation. This is because even after q_m having isolated them from the malicious ones in the current domain, they would still be in danger when being attacked in other domains.

Obviously, the most desirable solution to our attack-aware service provisioning problem is to quarantine all the malicious lightpaths while serve the remaining ones without unnecessary isolation. However, this would be extremely difficult provided that we cannot distinguish them precisely before the lightpaths have been set up and the actual attacks using some of them have been detected. Therefore, in this work, we try to leverage game theory to balance the tradeoff between spectrum utilization and domain security-level of the domain.

IV. Bayesian Game for Attack-aware Provisioning

We formulate a two-player Bayesian game to model the competition between q_m and q_{-m}, *i.e.*, the domain manager of the m-th domain and a user in an arbitrary neighbor domain of G^m, respectively. Apparently, q_{-m} can be either malicious or harmless, which is its private attribute. q_m is unaware of whether q_{-m} is malicious or not and only holds a probability of it being malicious.

We assume that before submitting its inter-domain request to q_m, q_{-m} chooses/suggests an ingress node in V_b^m, which is done by encoding the corresponding information in a request message and sending it to the domain manager of q_{-m} [5]. Therefore, if q_{-m} is malicious, it would prefer to choose the ingress node through which it can maximize the gain of its attack. Otherwise, q_{-m} would just report the ingress node of its inter-domain lightpath honestly. Hence, regardless of its type, *i.e.*, malicious or harmless, the pure strategies for q_{-m} are the ingress nodes in V_b^m. Considering the facts that the connecting points between two adjacent domains might not be too many and its domain manager might not allow q_{-m} to access all the border nodes at will, we assume that each time q_{-m} can select its ingress node from two candidates, *w.l.o.g.*, we denote them as $v_{b,1}^m$ and $v_{b,2}^m$.

Depending on the type of q_{-m}, the domain manager q_m should use different RSA algorithms to handle its inter-domain request. Specifically, q_m would be expected to apply an attack-aware RSA (Aa-RSA) algorithm on a malicious q_{-m}, while it would use a non-Aa-RSA algorithm for a harmless q_{-m}. Here, we assume that q_m would use the MDAa-RSA in [9] for a malicious q_{-m}. Specifically, MDAa-RSA tries to avoid the node/link sharing between lightpaths in R^{ex} and R^{in} with the best effort and would insert a sufficient guard-band (*e.g.*, 4 FS' or more) in between if the node/link sharing between these lightpaths cannot be avoided. Note that the aforementioned mechanism in MDAa-RSA is derived from analyzing the causes of intra/inter-channel crosstalk [9] and thus it helps to minimize the security threat to G^m due to the malicious q_{-m}. On the other hand, we assume that q_m would use the K-shortest-path and first-fit (KSP-FF) algorithm [28] with a relatively small guard-band (*i.e.*, 1 FS) for a harmless q_{-m}, *i.e.*, no additional spectrum isolation is applied even if the node/link sharing occurs. Therefore, the pure strategies for q_m would be the usages of MDAa-RSA and KSP-FF. Then, when the strategies of q_{-m} and q_m are both selected in a game, *i.e.*, the inter-domain request's ingress node and the RSA algorithm to serve it within G^m are both finalized, the actual RSA scheme to carry it within G^m can be obtained.

Based on the discussion above, we define the utility functions for q_{-m} and q_m with the following parameters.

Parameters:

- c_a: the total spectrum usage of the actual RSA scheme in G^m for q_{-m}.
- h_a: the hop-count of the path segment in the actual RSA.
- n_a: the number of FS' that the actual RSA scheme allocates on each related link.
- θ_a: the total security threat that the actual RSA scheme would cause to the existing lightpaths in G^m.
- α: the positive coefficient that applies to c_a in the utilities when MDAa-RSA has been used.
- β: the positive coefficient that applies to θ_a in the utilities when KSP-FF has been used.

After q_{-m} and q_m having selected their strategies in a game, the actual RSA scheme to carry the inter-domain request within G^m is obtained and thus c_a can be calculated as

$$c_a = n_a \cdot h_a.$$

Since a malicious lightpath can affect the lightpaths that are in R^{in} and share node/link with it (*i.e.*, within its attack range [9]), we quantify its security threat as the total legacy transmission capacity that it can affect, *i.e.*, defining θ_a as

$$\theta_a = \begin{cases} \sum\limits_{i \in \widehat{R^{in}}} C_i, & q_{-m} \text{ is malicious \& served with KSP-FF}, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where $\widehat{R^{in}}$ denotes the set of lightpaths that are in R^{in} and within the attack range of q_{-m} due to the actual RSA scheme, and C_i is the bandwidth requirement in FS' of such a lightpath. Hence, only if q_{-m} is malicious and it is served with KSP-FF (*i.e.*, being mistakenly treated as a harmless one by q_m), it can affect the legacy lightpaths in $\widehat{R^{in}}$. Otherwise, there is no security threat since either q_{-m} is harmless or it has already been quarantined by q_m with MDAa-RSA.

Fig. 1 provides an illustrative example on how to calculate c_a and θ_a. The domain topology of G^m is shown in Fig. 1(a) with V_b^m = {Node 1, Node 4}. In G^m, there are five lightpaths, *i.e.*, three in R^{in}, one in R^{lv}, and one in R^{ex}. Their routing paths are marked in different colors. We assume that each lightpath has a bandwidth requirement of 25 Gb/s and their spectrum utilizations are shown in Fig. 1(b). We assume that the two lightpaths in R^{in} using paths 1→2→6 and 2→6→5 are within the attack range of R_1^{ex}. Hence, if R_1^{ex} is malicious, we obtain $c_a = 2 \times 2 = 4$ FS' and $\theta_a = 2 + 2 = 4$ FS'. When q_{-m} and q_m have decided their strategies to use in a game, a strategy pair is formulated and thus the RSA solution is determined. For example, if there is another inter-domain lightpath (*i.e.*, R_2^{ex}) that needs to be provisioned with the destination as Node 5 and a bandwidth requirement of 25 Gb/s, its RSA schemes under each strategy pair are shown in Fig. 1. For the strategy pair (Node 1, KSP-FF), the RSA scheme is path 1→6→5 with FS-block $[6, 7]$. For the strategy pair (Node 1, MDAa-RSA), it is path 1→6→5 with FS-block $[9, 10]$. The strategy pairs in which R_2^{ex} selects Node 4 as its ingress node are also marked in Fig. 1.

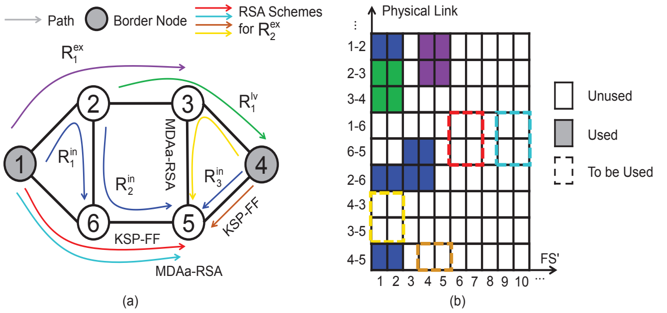


Fig. 1. Example on lightpath provisioning in a domain of MD-EON

With a specified RSA scheme, we can calculate the utilities of q_{-m} and q_m by analyzing their gains and costs. Table I summarizes the utility functions for each strategy pair. Here, we assume that before each game, the two players (*i.e.*, q_{-m} and q_m) have full knowledge about the values of the utility functions in Table I. This is because one of the basic requirements of game theory is that each player's utility function should be known to all the players in the game [10]. Otherwise, the game cannot be formulated since the players have no information to make their decisions on. Note that, as q_{-m} only needs to know c_a and θ_a to calculate the utility functions, a reasonable assumption would be that q_m reports c_a and θ_a before each game. Later on, our simulation results will show that with the game-assisted approach, q_m can improve its network performance, and thus there is a positive incentive for q_m to report c_a and θ_a before each game.

In Table I(a) (*i.e.*, q_{-m} is malicious), for the strategy pair ($v_{b,1}^m$, MDAa-RSA), the utilities of q_{-m} and q_m are both $-\alpha \cdot c_a$. Here, with Eq. (1), we can obtain the security threat of provisioning with MDAa-RSA as $\theta_a = 0$, and thus their utilities only contain the cost due to spectrum utilization. For the strategy pair ($v_{b,1}^m$, KSP-FF), the utilities become $(\beta \cdot \theta_a - c_a)$ and $(-\beta \cdot \theta_a - c_a)$ for q_{-m} and q_m, respectively. Specifically, a malicious q_{-m} can achieve a positive gain of $\beta \cdot \theta_a$ due to its attack, while q_m calculates its loss due to the attack as $\beta \cdot \theta_a$. The utilities in Table I(a) for the other two

TABLE I
UTILITY FUNCTIONS OF BAYESIAN GAME

(a) q_{-m} is malicious

	MDAa-RSA	KSP-FF
$v_{b,1}^m$	$-\alpha \cdot c_a$, $-\alpha \cdot c_a$	$(\beta \cdot \theta_a - c_a)$, $(-\beta \cdot \theta_a - c_a)$
$v_{b,2}^m$	$-\alpha \cdot c_a$, $-\alpha \cdot c_a$	$(\beta \cdot \theta_a - c_a)$, $(-\beta \cdot \theta_a - c_a)$

(b) q_{-m} is harmless

	MDAa-RSA	KSP-FF
$v_{b,1}^m$	$-\alpha \cdot c_a$, $-\alpha \cdot c_a$	$-c_a$, $-c_a$
$v_{b,2}^m$	$-\alpha \cdot c_a$, $-\alpha \cdot c_a$	$-c_a$, $-c_a$

strategy pairs can be analyzed similarly. Table I(b) shows the utilities when q_{-m} is harmless. Note that, since the actual RSA scheme changes with the ingress node, different strategy pairs would use different values of c_a and θ_a to get the utilities.

In the game, since both players are rational, they try to maximize their expected utilities. Specifically, q_m tries to minimize the security threat as well as the spectrum utilization, while if q_{-m} is malicious, it tries to maximize the security threat and minimize the spectrum utilization. Note that, if q_{-m} is harmless, the objectives of q_{-m} and q_m both becomes to minimize the spectrum utilization. With these objectives, q_{-m} and q_m need to find their best responses to the other's strategies, *i.e.*, determining the ingress node and the RSA algorithm for the inter-domain lightpath.

V. GAME-ASSISTED SERVICE PROVISIONING

In this section, we discuss how to solve the Bayesian game above to provision an inter-domain request from q_{-m}.

A. Bayesian Nash Equilibrium

As explained in the previous section, the players (*i.e.*, q_{-m} and q_m) need to find their mutual best responses to maximize their utilities. This actually can be achieved by analyzing the Nash equilibrium of the Bayesian game formulated in Section IV, since a Bayesian Nash equilibrium (BNE) represents a strategy profile in which neither q_{-m} nor q_m can increase its utility by adjusting the strategy unilaterally [10]. Note that, even when q_{-m} is malicious, it will report its ingress node honestly after each game, since changing its ingress node unilaterally would make q_{-m} deviate from its best response to the strategy of q_m and hence result in utility loss.

Theorem 1. *The Bayesian game formulated in Section IV has at least one mixed-strategy BNE.*

Proof: In the game, there are two players, *i.e.*, q_{-m} and q_m. With Table I, we can see that each player only has two pure strategies. Hence, the game is a finite one. As every finite Bayesian game has at least one mixed-strategy BNE [10], we prove the theorem. ■

In the following, we derive the general form of the BNE in the game and formulate a nonlinear programming model (NLP) to obtain it.

Parameters:

- λ: the priori probability that q_m believes that q_{-m} is malicious.
- $\mathbf{\Phi}_a^m$: the utility matrix of q_m under all the pure strategy pairs, if q_{-m} is malicious.
- $\mathbf{\Phi}_a^{-m}$: the utility matrix of q_{-m} under all the pure strategy pairs, if q_{-m} is malicious.
- $\mathbf{\Phi}_u^m$: the utility matrix of q_m under all the pure strategy pairs, if q_{-m} is harmless.
- $\mathbf{\Phi}_u^{-m}$: the utility matrix of q_{-m} under all the pure strategy pairs, if q_{-m} is harmless.
- L^{-m}: the value of the smallest element in $\mathbf{\Phi}_a^{-m}$ for a malicious q_{-m} or in $\mathbf{\Phi}_u^{-m}$ for a harmless q_{-m}.
- U^{-m}: the value of the largest element in $\mathbf{\Phi}_a^{-m}$ for a malicious q_{-m} or in $\mathbf{\Phi}_u^{-m}$ for a harmless q_{-m}.
- L^m: the value of the smallest element in $\mathbf{\Phi}_a^m$ and $\mathbf{\Phi}_u^m$.
- U^m: the value of the largest element in $\mathbf{\Phi}_a^m$ and $\mathbf{\Phi}_u^m$.

Variables:

- $\mathbf{s}^m$: the mixed-strategy vector $(s_1^m, s_2^m)^{\mathrm{T}}$ that indicates how q_m formulates its strategy. Specifically, s_1^m and s_2^m are the probabilities that q_m chooses to use MDAa-RSA and KSP-FF, respectively[1].
- $\mathbf{s}^a$: the mixed-strategy vector $(s_1^a, s_2^a)^{\mathrm{T}}$ that indicates how a malicious q_{-m} formulates its strategy. Specifically, s_1^a and s_2^a are the probabilities that q_{-m} chooses to access G^m from $v_{b,1}^m$ and $v_{b,2}^m$, respectively.
- $\mathbf{s}^u$: the mixed-strategy vector $(s_1^u, s_2^u)^{\mathrm{T}}$ that indicates how a harmless q_{-m} formulates its strategy. The definitions of s_1^u and s_2^u are similar as those of s_1^a and s_2^a.
- Ψ^m: the expected utility of q_m.
- Ψ^{-m}: the expected utility of q_{-m}.
- $\mathbf{z}^m$: the best response function of q_m.
- $\mathbf{z}^a$: the best response function of a malicious q_{-m}.
- $\mathbf{z}^u$: the best response function of a harmless q_{-m}.
- Γ^m: the optimal utility of q_m.
- Γ^{-m}: the optimal utility of q_{-m}.

Objectives:

The objective of q_{-m} is

$$Maximize \quad \Psi^{-m} = \begin{cases} (\mathbf{s}^a)^{\mathrm{T}} \mathbf{\Phi}_a^{-m} \mathbf{s}^m, & \text{malicious,} \\ (\mathbf{s}^u)^{\mathrm{T}} \mathbf{\Phi}_u^{-m} \mathbf{s}^m, & \text{harmless,} \end{cases} \tag{2}$$

where the expression of Ψ^{-m} depends on the actual type of q_{-m} since different types could lead to different decisions, *i.e.*, $\mathbf{s}^a$ might not be the same as $\mathbf{s}^u$.

The objective of q_m can be expressed as

$$Maximize \quad \Psi^m = \lambda \cdot (\mathbf{s}^a)^{\mathrm{T}} \mathbf{\Phi}_a^m \mathbf{s}^m + (1-\lambda) \cdot (\mathbf{s}^u)^{\mathrm{T}} \mathbf{\Phi}_u^m \mathbf{s}^m, \tag{3}$$

where the expected utility contains two parts, each of which is weighted by the corresponding priori probability. The first part is for when q_m believes that q_{-m} is malicious, while the second part is the other way around.

With the objectives in Eqs. (2)-(3), and we can get the best

[1] Here, the superscript T is the transposition operator.

response functions as

$$\begin{cases} \mathbf{z}^a(\mathbf{s}^m) = \arg\max_{\mathbf{s}^a} \ \Psi^{-m}, & \text{malicious,} \\ \mathbf{z}^u(\mathbf{s}^m) = \arg\max_{\mathbf{s}^u} \ \Psi^{-m}, & \text{harmless.} \end{cases} \tag{4}$$

$$\mathbf{z}^m(\mathbf{s}^a, \mathbf{s}^u) = \arg\max_{\mathbf{s}^m} \ \Psi^m. \tag{5}$$

Specifically, given a mixed-strategy of q_m (*i.e.*, $\mathbf{s}^m$), q_{-m} uses Eq. (4) to obtain its best response (*i.e.*, $\mathbf{z}^a$ or $\mathbf{z}^u$). Similarly, q_m leverages Eq. (5) to get its best response $\mathbf{z}^m$. Then, by definition, BNE is expressed as $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$, if Eqs. (4)-(5) can be satisfied simultaneously. In order to figure out $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$, we adopt the method in [40], which reduces the problem of finding a BNE to solving the optimization of the NLP below.

Objective:

$$Minimize \quad f = |\Gamma^m - \Psi^m| + |\Gamma^{-m} - \Psi^{-m}|, \tag{6}$$

where f is the summation of two items that denote the gaps between the optimal utility and the expected utility of q_m and q_{-m}. By minimizing f to 0, we obtain a BNE.

Constraints:

$$\begin{cases} \mathbf{\Phi}_a^{-m}\mathbf{s}^m \leq (\Gamma^{-m}, \Gamma^{-m})^{\mathrm{T}}, & \text{malicious,} \\ \mathbf{\Phi}_u^{-m}\mathbf{s}^m \leq (\Gamma^{-m}, \Gamma^{-m})^{\mathrm{T}}, & \text{harmless,} \end{cases} \tag{7}$$

$$\lambda \cdot (\mathbf{s}^a)^{\mathrm{T}}\mathbf{\Phi}_a^m + (1-\lambda) \cdot (\mathbf{s}^u)^{\mathrm{T}}\mathbf{\Phi}_u^m \leq (\Gamma^m, \Gamma^m). \tag{8}$$

Eqs. (7)-(8) ensure that none of the players can increase its utility by changing its own strategy.

$$\Gamma^{-m} \in [L^{-m}, U^{-m}], \tag{9}$$

$$\Gamma^m \in [L^m, U^m]. \tag{10}$$

Eqs. (9)-(10) ensure that Γ^{-m} and Γ^m are within right ranges.

$$\sum_{i=1}^{2} s_i^a = \sum_{i=1}^{2} s_i^u = \sum_{i=1}^{2} s_i^m = 1, \tag{11}$$

$$s_i^m, s_i^a, s_i^u \in [0, 1], \quad \forall i = 1, 2. \tag{12}$$

Eqs. (11)-(12) ensure regularity and nonnegative constraints.

We then use the sequential quadratic programming based quasi-Newton (SQP-qN) method [41] to solve the NLP. Note that the performance of this method would be affected by the initial searching point, which means that we will find the BNE that is the closest to the initial searching point [41]. To handle this issue, we design *Algorithm* 1. *Lines* 1-2 are for the initialization. Here, by saying a "pure strategy profile", we mean that the elements in $\mathbf{s}^a$, $\mathbf{s}^u$, and $\mathbf{s}^m$ can only be 0 or 1, *i.e.*, q_m or q_{-m} selects one of its strategies deterministically. The for-loop that covers *Lines* 3-8 uses all the pure strategy profiles as the initial searching points to solve the NLP for BNEs. *Lines* 4-5 calculate an initial searching point with a pure strategy profile and input it to the NLP. The NLP is solved in *Line* 6 with SQP-qN for a BNE. *Line* 7 stores the obtained BNE. With *Lines* 9-13, we try to get the best BNE as the one with a pure strategy profile, and only when no pure strategy BNE exists, we select a mixed-strategy one. Since either q_m or q_{-m} only has two pure strategies, the search space defined by $|\mathbf{S}| = 8$ is very small and thus the complexity of *Algorithm* 1 only depends on that of using SQP-qN to solve the NLP, which has been verified as time-efficient in [40].

Algorithm 1: Searching for BNE

```
1  calculate utility matrices $\mathbf{\Phi}_a^m$, $\mathbf{\Phi}_a^{-m}$, $\mathbf{\Phi}_u^m$, and $\mathbf{\Phi}_u^{-m}$;
2  store all pure strategy profiles $(\mathbf{s}^a, \mathbf{s}^u, \mathbf{s}^m)$ in $\mathbf{S}$;
3  for each $(s^a, s^u, s^m) \in S$ do
4      calculate $\Psi^m$ and $\Psi^{-m}$ with Eqs. (2)-(3);
5      input $(\mathbf{s}^a, \mathbf{s}^u, \mathbf{s}^m)$, $\Psi^m$ and $\Psi^{-m}$ to the NLP;
6      solve the NLP with SQP-qN for a $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$;
7      store $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$ in $\mathbf{Z}$;
8  end
9  if $S \cap Z = \emptyset$ then
10     select $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$ from $\mathbf{Z}$ randomly;
11 else
12     select $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$ from $\mathbf{S} \cap \mathbf{Z}$ randomly;
13 end
14 return $(\mathbf{z}^a, \mathbf{z}^u, \mathbf{z}^m)$ as the best BNE;
```

B. Game-assisted Service Provisioning

In addition to those in R^{ex}, we also need to provision the lightpaths in R^{in} and R^{lv} in G^m. *Algorithm* 2 shows the procedure of our proposed game-assisted service provisioning. *Lines* 1-2 are for the initialization. The for-loop that covers *Lines* 3-19 is to provision all the requests. Specifically, for various types of lightpaths, we adopt different RSA algorithms, *i.e.*, MDAa-RSA for R^{in}, KSP-FF for R^{lv}, and the game-assisted RSA (Ga-RSA) for R^{ex}. In *Lines* 13-19, we try to provision each lightpath using the obtained RSA scheme. The complexity of MDAa-RSA is $O_1 = O(K \cdot |V_b^m|^2 \cdot (|\mathbf{R}| + |V^m| \cdot |E^m| + F \cdot (|V^m| + |E^m|)))$ according to [9]. Hence, if we denote the complexity of *Algorithm* 1 as O_2, the complexity of *Algorithm* 2 would be $|\mathbf{R}| \cdot \max(O_1, O_2)$.

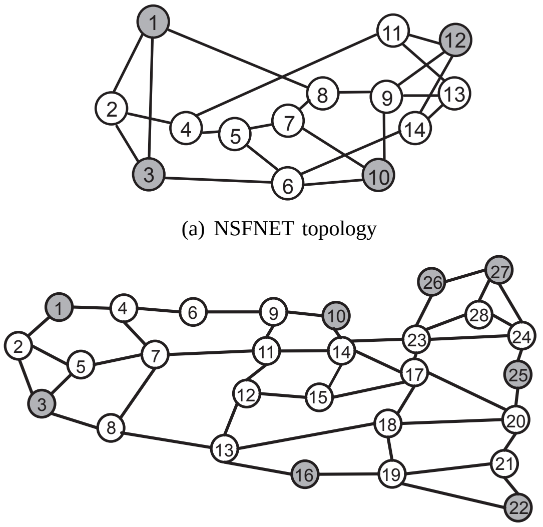
VI. Performance Evaluation

In this section, we evaluate the proposed game-assisted service provisioning scheme with numerical simulations. In order to obtain sufficient statistical accuracy, we get each data point by averaging the results from five independent simulations. The simulation environment is MATLAB R2014b running on a computer with 3.20 GHz Intel Core i5-4570M CPU and 8 GB RAM.

We use two topologies as G^m in the simulations, *i.e.*, the NSFNET and US Backbone topologies shown in Fig. 2. In each topology, we mark the border nodes as grey. The capacity of each fiber link is 4.475 THz in C-band, corresponding to 358 FS'. For the dynamic service provisioning, all the requests come and leave on-the-fly, which follows the Poisson traffic model. The three types of lightpaths, *i.e.*, R^{in}, R^{lv} and R^{ex}, are generated according to the ratio of $[2:1:1]$. For each request, its source(s) and destination(s) are randomly selected according to the network model described in Section III and its bandwidth requirement is uniformly distributed within $[12.5, 250]$ Gb/s. Within R^{ex}, some are malicious

Algorithm 2: Provisioning Procedure (Ga-RSA)

```
classify requests in $\mathbf{R}$ into $R^{in}$, $R^{lv}$ and $R^{ex}$;
sort requests in descending order of bandwidth
requirement;
for each request $R_i \in \mathbf{R}$ do
    if $R_i$ is an $R^{in}$ then
        apply MDAa-RSA to obtain the RSA scheme;
    else
        if $R_i$ is an $R^{lv}$ then
            apply KSP-FF to obtain the RSA scheme;
        else
            solve the Bayesian game with Algorithm 1
            to obtain the RSA scheme;
        end
    end
    if no feasible RSA scheme can be found then
        mark $R_i$ as blocked;
    else
        serve $R_i$ using the obtained RSA scheme;
        update the network status;
    end
end
```



(a) NSFNET topology

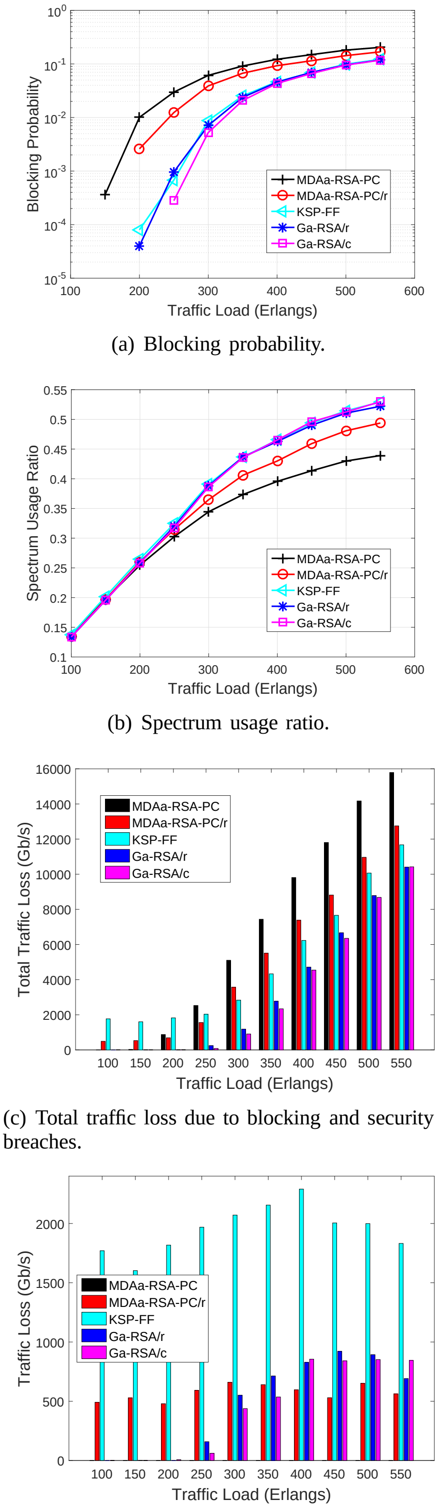
(b) US Backbone topology

Fig. 2. Domain topologies with border nodes marked as grey.

lightpaths while the others are harmless ones. For the inter-domain lightpaths in R^{ex}, we denote the ratio of malicious to total as η. Note that, in the worst-case scenario, the domain manager q_m has no prior knowledge about η and can only take random guesses when serving inter-domain lightpaths. Hence, the belief that q_m holds of a q_{-m} being malicious would be 0.5, *i.e.*, $\lambda = 0.5$. We name our Ga-RSA in this worst-case scenario as Ga-RSA/r. On the other hand, the ideal scenario would be that q_m knows exactly about whether a lightpath in R^{ex} is malicious or harmless when serving it, and we denote the Ga-RSA in this scenario as Ga-RSA/c. With these two scenarios, we can investigate the impact of λ on our Ga-RSA. We use the MDAa-RSA-PC algorithm in [9] as the benchmark. MDA-RSA-PC isolates all the lightpaths in R^{in} from those in R^{ex} with sufficient spectrum isolation, no matter whether the inter-domain lightpaths in R^{ex} are malicious or not, and when doing so, MDA-RSA-PC can also reduce the node/link sharing among the lightpaths in R^{in} and R^{ex} to save spectrum utilization. To make the comparisons more thorough, we incorporate a modified version of MDAa-RSA-PC (MDAa-RSA-PC/r) in which q_m would isolate an inter-domain lightpath in R^{ex} from those in R^{in} with a probability of 0.5 (*i.e.*, using random guesses). Also, KSP-FF is used as a non-attack-aware benchmark. Note that, even though we assume that at the time of each game, q_m does not know the type of q_{-m}, the malicious lightpaths would become known to q_m after they have actually launched attacks. Hence, when serving subsequent intra-domain requests, q_m will isolate them from the known-malicious ones.

We first set $\eta = 0.02$ and perform the simulations. Fig. 3 shows the simulation results in the NSFNET topology. Fig. 3(a) shows the results on blocking probability, which is defined as the ratio of blocked to total lightpath requests. We can see that compared with MDAa-RSA-PC/r and MDAa-RSA-PC, Ga-RSA achieves much lower blocking probability. Note that, in MDAa-RSA-PC, the strict defense scheme is applied to quarantine each inter-domain lightpath (*i.e.*, R_i^{ex}) from all the intra-domain ones, while MDAa-RSA-PC/r would take a random guess to decide whether R_i^{ex} should be quarantined or not. In Ga-RSA, the belief of R_i^{ex} being malicious is just used to assist the gaming procedure, and the provisioning scheme is then determined for R_i^{ex} by analyzing the utility functions. Specifically, based on the BNE in the game we formulated, q_m can find the best strategy to serve each inter-domain lightpath, no matter q_{-m} is malicious or not. Hence, the intelligent provisioning scheme helps to lower blocking probability in Ga-RSA. Moreover, since we design the Bayesian game to consider the total spectrum usage (*i.e.*, c_a) in the players' utility functions, Ga-RSA can achieve comparable blocking probability, when being compared with the non-attack-aware benchmark KSP-FF. Fig. 3(b) shows the results on spectrum usage ratio, *i.e.*, the average ratio of used to total FS' in the domain. We observe that Ga-RSA based approaches provide much higher spectrum usage ratios than MDAa-RSA-PC and MDAa-RSA-PC/r do when the traffic load is relatively high (*i.e.*, $\geq$ 300 Erlangs). This attributes to the fact that Ga-RSA wastes less spectra on isolating intra-domain requests from harmless inter-domain ones, which leads to less spectrum fragmentation in the domain. Hence, as Ga-RSA can provision more lightpaths, it produces a higher spectrum usage ratio.

Note that, in addition to request blocking, security breaches caused by malicious lightpaths (*i.e.*, θ_a in Eq. (1) in Section IV) would also result in traffic loss. Hence, in Figs. 3(c) and 3(d), we show the total traffic loss and the traffic loss due to security breaches, respectively. We observe that Ga-RSA based approaches provide the least total traffic loss. Specifically, compared with MDAa-RSA-PC/r and MDAa-RSA-PC, they benefit from much less request blocking while compared with KSP-FF, they have the advantage of much less security breaches. This verifies the effectiveness of Ga-RSA on balancing the tradeoff between spectrum usage and



(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 3. Simulation results in NSFNET topology ($\eta = 0.02$).

the level of security. In Fig. 3, we also find that Ga-RSA/c only outperforms Ga-RSA/r slightly in terms of blocking probability and total traffic loss. This observation suggests that the choice of λ indeed affects the performance of Ga-RSA, but the performance loss would be acceptable if q_m just follows the worst-case scenario to take random guesses.

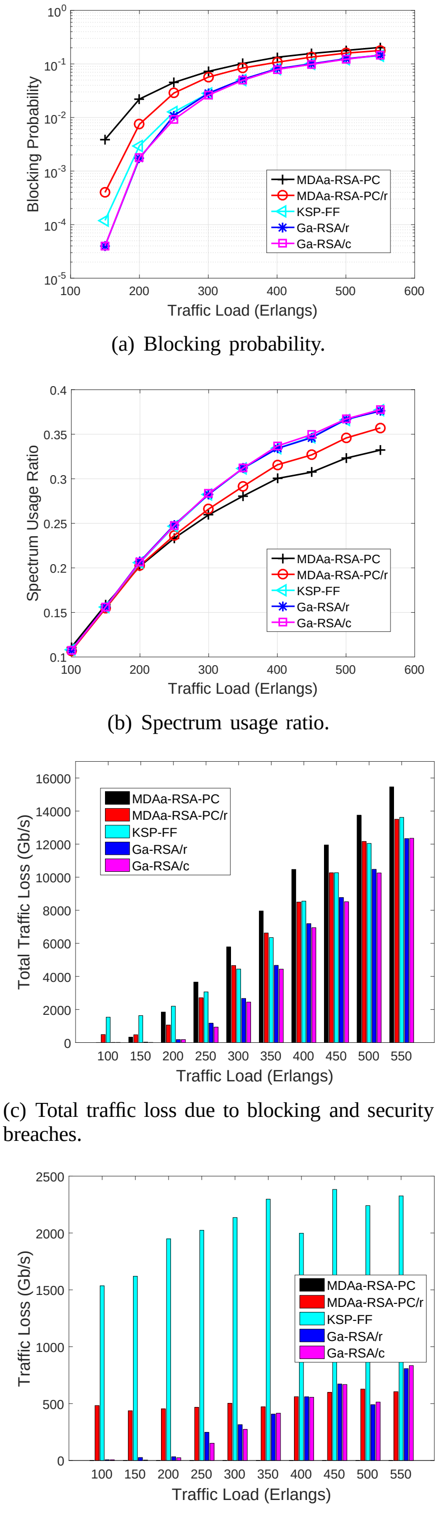
Table II lists the running time, from which we can see that Ga-RSA takes more time than the benchmarks due to the time spent on solving the NLP. It is also interesting to notice that the running time of Ga-RSA would not always increase with the traffic load. This is because when the traffic load increases, some of the strategy pairs would become infeasible due to the crowded spectrum utilization and to certain extent, this might make solving the NLP unnecessary since only one strategy pair is feasible for q_m or q_{-m}. We can see that the running time of Ga-RSA is already relatively short. However, according to [42], the very fast lightpath setup in optical networks might require a path computation and setup time that is less than 5 msec. In our future work, we will further reduce Ga-RSA's running time to meet this stringent requirement, by optimizing the algorithm's implementation, realizing it with C/C++, and using a more powerful server for computation.

The results in the US Backbone topology are illustrated in Fig. 4 and Table III, where they follow the similar trends as those in the NSFNET topology. We can see that the performance gap of total traffic loss between Ga-RSA and MDAa-RSA-PC becomes smaller. This is because for a lightpath in R^{ex}, it is more difficult for Ga-RSA to provision it with MDAa-RSA in a larger topology, and hence Ga-RSA would use KSP-FF more often, which leads to more traffic loss due to security breaches.

TABLE II
RUNNING TIME PER REQUEST IN NSFNET TOPOLOGY.

Traffic of	Running Time (Seconds)			
(Erlangs)	Ga-RSA/c	Ga-RSA/r	MDAa-RSA-PC (/r)	KSP-FF
150	0.152	0.156	0.045 (0.013)	0.004
250	0.130	0.136	0.045 (0.014)	0.006
350	0.070	0.069	0.052 (0.011)	0.008
450	0.061	0.060	0.053 (0.010)	0.009
550	0.059	0.060	0.049 (0.010)	0.010

As the security issue of Ga-RSA would become worse with the increase of η (*i.e.*, more inter-domain lightpaths are malicious), we conduct more simulations with different values of η to investigate when its advantage on spectrum utilization would disappear. The simulation results in the NSFNET and US Backbone topologies are shown in Figs. 5-6. Here, we compare the performance of Ga-RSA/r and MDAa-RSA-PC(/r), and denote the Ga-RSA/r and MDAa-RSA-PC/r based approaches with the format of "Ga-RSA/r/η" and "MDAa-RSA-PC/r/η". In Figs. 5(a) and 6(a), the blocking probabilities from Ga-RSA/r still outperform those from MDAa-RSA-PC(/r) under the same values of η. Similarly, Figs. 5(b) and 6(b) demonstrate the effectiveness of Ga-RSA/r on improving the spectrum usage ratio under the same values of η. Nevertheless, in Figs. 5(c) and 6(c), we find that the total traffic loss from Ga-RSA/r increases significantly with η and can become comparable to or even higher than those from MDAa-RSA-PC with $\eta = 0.15$. Hence, for a relatively high η, the security breaches increase and cannot be overlooked in Ga-RSA. This suggests that in a relatively safe MD-EON, Ga-RSA can balance the spectrum utilization and security-related traffic loss better than the benchmarks, but when the MD-EON



(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 4. Simulation results in US Backbone topology ($\eta = 0.02$).

becomes as dangerous as $\eta \geq 0.15$, it might sacrifice security breaches too much for saving spectrum utilization.

All the results above are obtained under the assumption that the domain manager could detect the attacks from a malicious lightpath in R^{ex}. To further verify the effectiveness of Ga-RSA, we consider a more realistic scenario in which the domain manager can only detect a portion of malicious inter-domain lightpaths. We compare the performance of Ga-RSA/r and MDAa-RSA-PC/r with three detection ratios, *i.e.*, 100%, 90% and 80%. Figs. 7(a) and 8(a) indicate that the blocking probability from Ga-RSA/r increases slightly with the detection ratio. This is because more spectra are needed to isolate subsequent intra-domain lightpaths from known-malicious inter-domain ones when the detection ratio is higher. The results in Figs. 7(b) and 8(b) verify the effectiveness of Ga-RSA/r on improving the spectrum usage. As for the total traffic loss and security breaches in Figs. 7(c) and 8(c), we can see that the superiority of Ga-RSA/r remains.

TABLE III
RUNNING TIME PER REQUEST IN US BACKBONE TOPOLOGY.

Traffic	Running Time (Seconds)			
(Erlangs)	Ga-RSA/c	Ga-RSA/r	MDAa-RSA-PC (/r)	KSP-FF
150	0.145	0.150	0.050 (0.013)	0.005
250	0.100	0.102	0.058 (0.013)	0.007
350	0.074	0.073	0.061 (0.013)	0.009
450	0.065	0.068	0.061 (0.011)	0.010
550	0.063	0.065	0.063 (0.011)	0.010

VII. CONCLUSION

This paper studied the problem of attack-aware service provisioning in one domain of an MD-EON. We considered a realistic scenario that does not treat all the inter-domain lightpaths as malicious ones, and tried to arrange the lightpaths' RSA schemes with the help of game theory to balance the spectrum utilization and security-level of the domain well. Specifically, we defined a two-player Bayesian game to represent the provisioning procedure for each inter-domain request, and designed the game strategies and utility functions for the players (*i.e.*, the domain manager and the user from other domains). With the game model, we proposed a game-assisted RSA (Ga-RSA) to achieve attack-aware service provisioning efficiently. The proposed algorithm was evaluated with extensive simulations and the results suggested that Ga-RSA could balance the tradeoff between spectrum utilization and traffic loss due to security breaches well in a relatively safe MD-EON.

ACKNOWLEDGMENTS

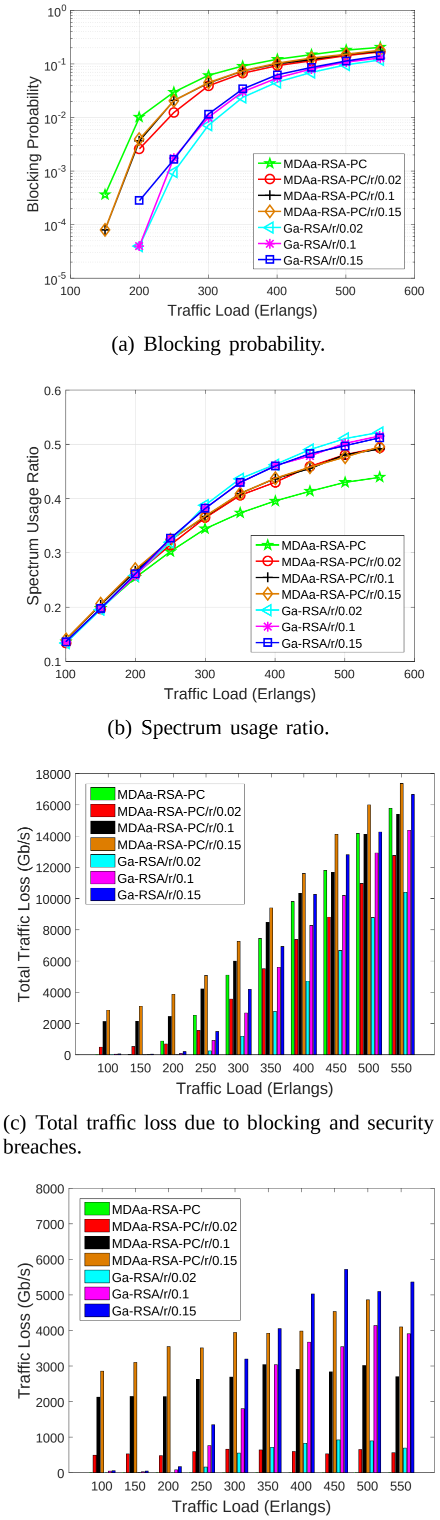
This work was supported in part by the NSFC Project 61371117, Natural Science Research Project for Universities in Anhui (KJ2014ZD38), and the Strategic Priority Research Program of the CAS (XDA06011202).

REFERENCES

[1] P. Lu *et al.*, "Highly-efficient data migration and backup for big data applications in elastic optical inter-datacenter networks," *IEEE Netw.*, vol. 29, pp. 36–42, Sept./Oct. 2015.

[2] F. Ji *et al.*, "Dynamic p-cycle protection in spectrum-sliced elastic optical networks," *J. Lightw. Technol.*, vol. 32, pp. 1190–1199, Mar. 2014.

[3] W. Fang *et al.*, "Joint defragmentation of optical spectrum and IT resources in elastic optical datacenter interconnections," *J. Opt. Commun. Netw.*, vol. 7, pp. 314–324, Mar. 2015.



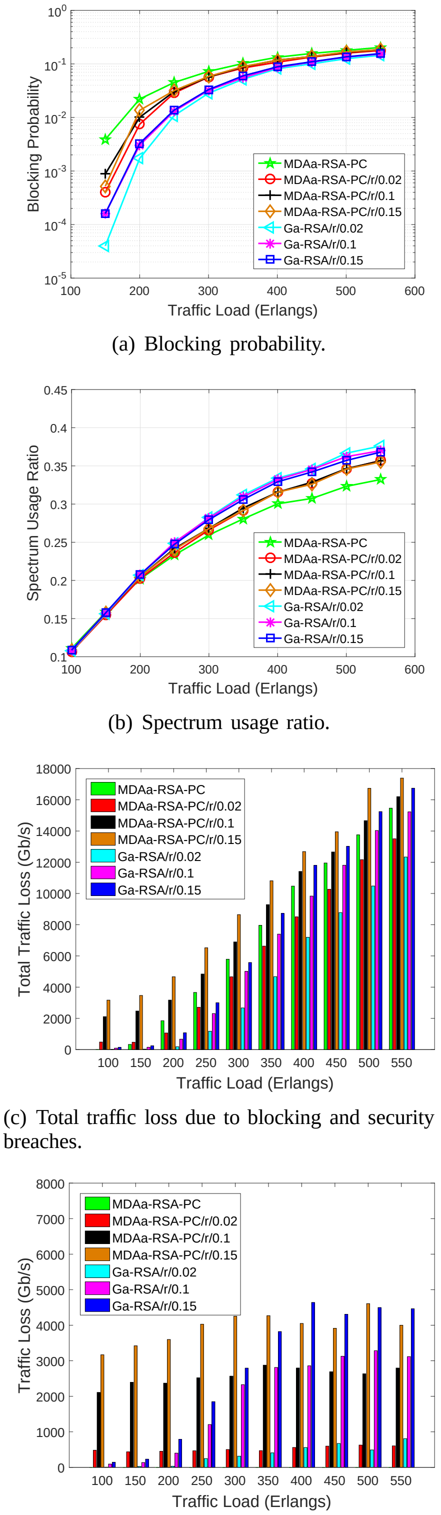
(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 5. Simulation results in NSFNET topology with different values of η.



(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 6. Simulation results in US Backbone topology with different values of η.

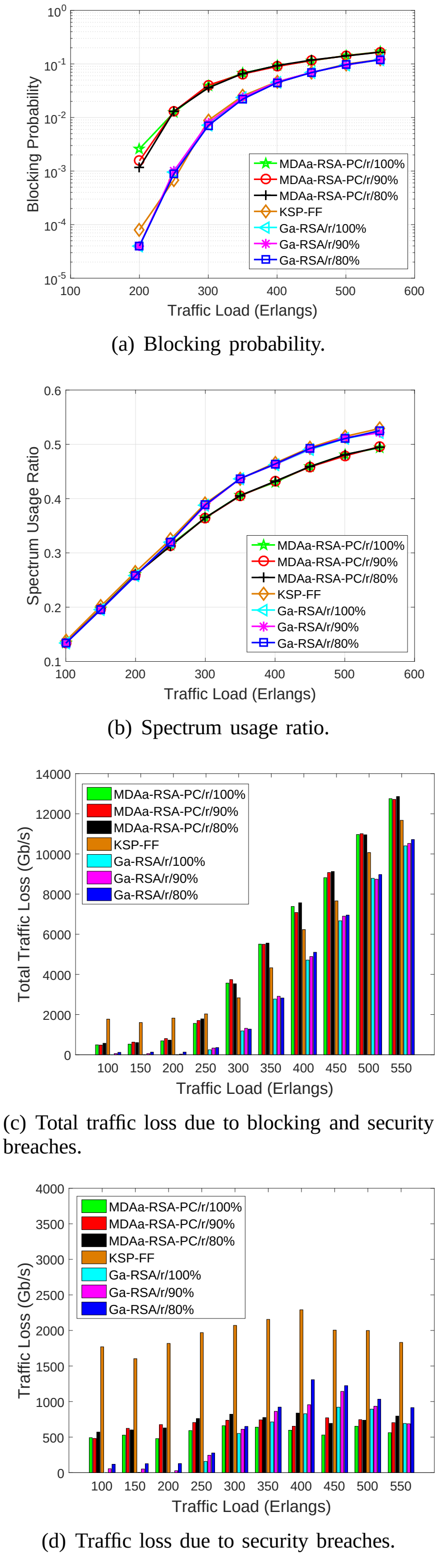
[4] R. Casellas *et al.*, "Control and management of flexi-grid optical networks with an integrated stateful path computation element and OpenFlow controller," *J. Opt. Commun. Netw.*, vol. 5, pp. A57–A65, Oct. 2013.

[5] Z. Zhu *et al.*, "Demonstration of cooperative resource allocation in an OpenFlow-controlled multidomain and multinational SD-EON testbed," *J. Lightw. Technol.*, vol. 33, pp. 1508–1514, Apr. 2015.

[6] X. Chen *et al.*, "Incentive-driven bidding strategy for brokers to compete for service provisioning tasks in multi-domain SD-EONs," *J. Lightw. Technol.*, vol. 34, pp. 3867–3876, Aug. 2016.

[7] Z. Zhu *et al.*, "Jitter and amplitude noise accumulations in cascaded all-optical regenerators," *J. Lightw. Technol.*, vol. 26, pp. 1640–1652, Jun. 2008.

[8] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*,



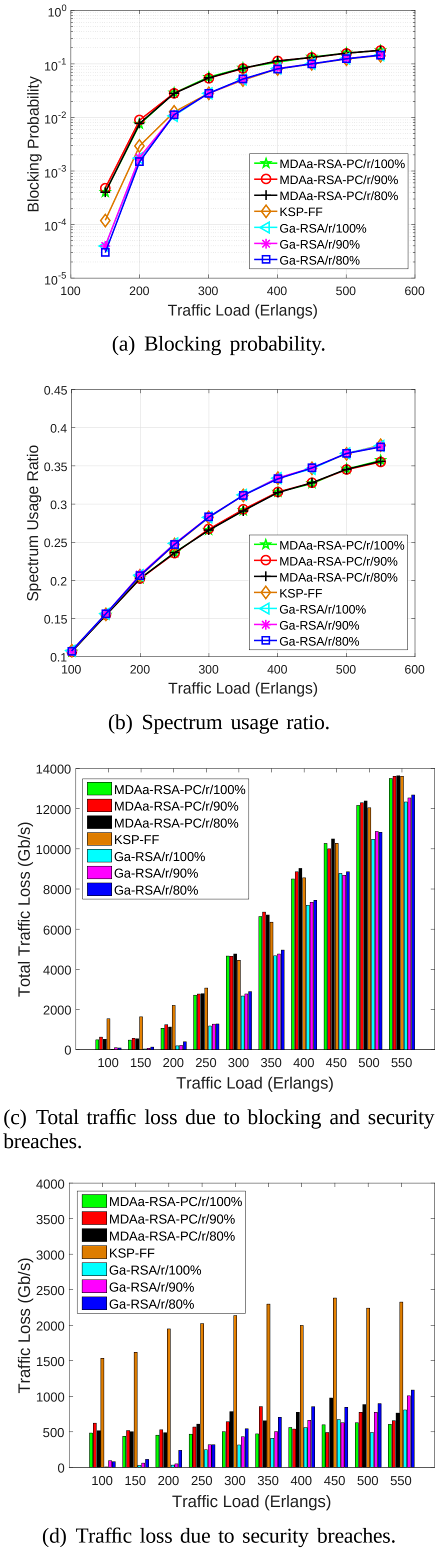
(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 7. Simulation results in NSFNET topology with different detection ratios ($\eta = 0.02$).



(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 8. Simulation results in US Backbone topology with different detection ratios ($\eta = 0.02$).

vol. 54, pp. 110–117, Aug. 2016.

[9] J. Zhu, B. Zhao, W. Lu, and Z. Zhu, "Attack-aware service provisioning to enhance physical-layer security in multi-domain EONs," *J. Lightw. Technol.*, vol. 34, pp. 2645–2655, Jun. 2016.

[10] Z. Han, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge University Press, 2012.

[11] K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection prevention," in *Proc. of MILCOM 2004*, pp. 711–716, Oct. 2004.

[12] C. Mas, I. Tomkos, and O. Tonguz, "Failure location algorithm for transparent optical networks," *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 1508–1519, Aug. 2005.

[13] R. Rejeb, M. Leeson, and R. Green, "Fault and attack management in all-optical networks," *IEEE Commun. Mag.*, vol. 44, pp. 79–86, Nov.

2006.

[14] M. Fok, Z. Wang, Y. Deng, and P. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 725–736, Sept. 2011.

[15] X. Chen *et al.*, "Flexible availability-aware differentiated protection in software-defined elastic optical networks," *J. Lightw. Technol.*, vol. 33, pp. 3872–3882, Sept. 2015.

[16] M. Furdek, N. Skorin-Kapov, and M. Grbac, "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation," *J. Opt. Commun. Netw.*, vol. 2, pp. 1000–1009, Nov. 2010.

[17] N. Skorin-Kapov, J. Chen, and L. Wosinska, "A new approach to optical networks security: Attack-aware routing and wavelength assignment," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 750–760, Jun. 2010.

[18] K. Manousakis and G. Ellinas, "Attack-aware planning of transparent optical networks," *Opt. Switch. Netw.*, vol. 19, pp. 97–109, Jan. 2016.

[19] H. Wu, F. Zhou, Z. Zhu, and Y. Chen, "Interference-and-security-aware distance spectrum assignment in elastic optical networks," in *Proc. of NOC 2016*, pp. 100–105, Jul. 2016.

[20] C. Chen *et al.*, "Demonstration of OpenFlow-controlled cooperative resource allocation in a multi-domain SD-EON testbed across multiple nations," in *Proc. of ECOC 2014*, pp. 1–3, Sept. 2014.

[21] S. Hong *et al.*, "Survivable virtual topology design in IP over WDM multi-domain networks," in *Proc. of ICC 2015*, pp. 5150–5155, May 2015.

[22] A. Castro *et al.*, "Brokered orchestration for end-to-end service provisioning across heterogeneous multi-operator (Multi-AS) optical networks," *J. Lightw. Technol.*, vol. 34, pp. 5391–5400, Dec. 2016.

[23] Z. Zhu *et al.*, "OpenFlow-assisted online defragmentation in single-/multi-domain software-defined elastic optical networks," *J. Opt. Commun. Netw.*, vol. 7, pp. A7–A15, Jan. 2015.

[24] K. Christodoulopoulos, I. Tomkos, and E. Varvarigos, "Elastic bandwidth allocation in flexible OFDM-based optical networks," *J. Lightw. Technol.*, vol. 29, pp. 1354–1366, May 2011.

[25] L. Gong, X. Zhou, W. Lu, and Z. Zhu, "A two-population based evolutionary approach for optimizing routing, modulation and spectrum assignments (RMSA) in O-OFDM networks," *IEEE Commun. Lett.*, vol. 16, pp. 1520–1523, Sept. 2012.

[26] X. Zhou, W. Lu, L. Gong, and Z. Zhu, "Dynamic RMSA in elastic optical networks with an adaptive genetic algorithm," in *Proc. of GLOBECOM 2012*, pp. 2912–2917, Dec. 2012.

[27] W. Lu *et al.*, "Dynamic multi-path service provisioning under differential delay constraint in elastic optical networks," *IEEE Commun. Lett.*, vol. 17, pp. 158–161, Jan. 2013.

[28] Z. Zhu, W. Lu, L. Zhang, and N. Ansari, "Dynamic service provisioning in elastic optical networks with hybrid single-/multi-path routing," *J. Lightw. Technol.*, vol. 31, pp. 15–22, Jan. 2013.

[29] Y. Yin, M. Zhang, Z. Zhu, and S. Yoo, "Fragmentation-aware routing, modulation and spectrum assignment algorithms in elastic optical networks," in *Proc. of OFC 2013*, pp. 1–3, Mar. 2013.

[30] X. Liu, L. Gong, and Z. Zhu, "Design integrated RSA for multicast in elastic optical networks with a layered approache," in *Proc. of GLOBECOM 2013*, pp. 2346–2351, Dec. 2013.

[31] S. Ma *et al.*, "Demonstration of online spectrum defragmentation enabled by OpenFlow in software-defined elastic optical networks," in *Proc. of OFC 2014*, pp. 1–3, Mar. 2014.

[32] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. of GameNets 2006*, pp. 1–12, Oct. 2006.

[33] D. Niyato and E. Hossain, "Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of Nash equilibrium, and collusion," *IEEE J. Sel. Areas Commun*, vol. 26, pp. 192–202, Jan. 2008.

[34] G. Shrimali, A. Akella, and A. Mutapcic, "Cooperative interdomain traffic engineering using Nash bargaining and decomposition," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 341–352, Apr. 2010.

[35] O. Kabranov, A. Yassine, and D. Makrakis, "Game theoretic pricing and optimal routing in optical networks," in *Proc. of ICCT 2003*, pp. 604–607, Apr. 2003.

[36] E. Bampas, A. Pagourtzis, G. Pierrakos, and K. Potika, "On a noncooperative model for wavelength assignment in multifiber optical networks," *IEEE/ACM Trans. Netw.*, vol. 20, pp. 1125–1137, Aug. 2012.

[37] K. Loja, J. Szigeti, and T. Cinkler, "Inter-domain routing in multi-provider optical networks: game theory and simulations," in *Proc. of NGI 2005*, pp. 157–164, Apr. 2005.

[38] Z. Zhu *et al.*, "Energy-efficient translucent optical transport networks with mixed regenerator placement," *J. Lightw. Technol.*, vol. 30, pp. 3147–3156, Oct. 2012.

[39] J. Zhu *et al.*, "Service provisioning with energy-aware regenerator allocation in multi-domain EONs," in *Proc. of GLOBECOM 2015*, pp. 1–6, Dec. 2015.

[40] B. Chatterjee, "An optimization formulation to compute Nash equilibrium in finite games," in *Proc. of ICM2CS 2009*, pp. 1–5, Dec. 2009.

[41] R. Fletcher, *Practical Methods of Optimization*. John Wiley & Sons, 2004.

[42] A. Malis, B. Wilson, G. Clapp, and V. Shukla, "Requirements for very fast setup of GMPLS label switched paths (LSPs)," *RFC 7709*, Nov. 2015. [Online]. Available: https://tools.ietf.org/html/rfc7709